

## Introducing eSafe Content Security

eSafe is a proactive web content security solution that provides strong security with the high capacity and reliability needed to effectively protect against known and unknown threats. eSafe provides transparent deep-web content inspection with effective speeds starting at 5 million fully inspected web pages per hour.

eSafe proactively protects against all content threats - spyware, Trojans, zombie-bots, viruses, worms, phishing, spam, Web 2.0 client-attacks; monitors HTTP and FTP and webmail, and optionally HTTPS, SMTP, and POP3. eSafe also and controls usage of various unauthorized applications in 19 categories including IM, P2P, tunneling, remote PC, etc.

eSafe reveals web usage, threats, and abuse in real-time including: real-time outbound and inbound threats containment; centralized content security threats assessment; web usage monitoring and granular policy enforcement.

### eSafe Highlights and Unique Features

- Proactive protection against:
  - Zero-day exploits in Web pages
  - Known and suspicious malicious VB and Java scripts Web / Web 2.0 pages
  - Untrusted ActiveX objects
- 4-layer spyware and web-surfing attack defense
- Goes beyond HTTP/FTP whole-file signatures
- Full HTML inspection in all web pages
- Selective stripping of definite and potentially malicious code within HTML pages
- Non-proxy, packet by packet content inspection and HTML modification capability
- The only product inspecting all web page content at tens of megabits per second
- Outbound and inbound application traffic blocking and enforcement

### Unique eSafe Capabilities

#### **Full web page content inspection at tens of megabits per second**

eSafe blocks malicious code, scripts, exploits and more. Other products only block downloaded files. The Spyware epidemic, enforced by phishing and targeted attacks, infect computers when users access infected web sites, strengthens the need for such capabilities, still lacking in many small and medium organizations, and surprisingly only implemented in 15-20% of large enterprises.

#### **Non-proxy, packet by packet content inspection and HTML modification**

eSafe features the patented non-proxy NitroInspection™ technology - transparently inspecting all Web surfing content. NitroInspection filters the relevant HTTP traffic for inspection out of the entire Internet traffic, and effectively handles 50Mbps of Web surfing content, fully inspected, including all the HTML page content. This is 5-10 times the capacity of any competing product.

eSafe is even faster than most simplistic gateway antivirus products. These products do not inspect all Web content but only downloaded files such as EXE, ZIP. Downloaded files constitute to probably less than 3% of the HTTP traffic, and limiting inspection to this is definitely not enough.

The packet-by-packet inspection method used by eSafe's NitroInspection is free from the limitations found in proxy solutions. Web pages are inspected as the packets arrive. There is no need for the entire HTML file to be downloaded and cached before inspection, if at all, as a result the user

experience is completely the same as with no inspection. Latency is a low 15-18ms for any inspected Web page, which is unnoticeable by all means.

The packet-by-packet inspection method also enables eSafe to be the only product which can dynamically and transparently modify Web surfing content when suspicious or potentially malicious HTML content is detected in Web pages, only stripping the suspicious or unsafe parts, leaving the Web page intact, and fully functional. All other competing solutions revert to blocking the entire Web page, creating user dissatisfaction, or they do not modify anything and compromise security.

## **Full inspection of all web-email traffic and HTTP elements in regular email**

Modern email security cannot be complete without HTTP email inspection for two important reasons:

1. Email messages arriving in SMTP, POP3, or IMAP, are constructed in HTML and often contain elements which are downloaded from the Web via HTTP when viewing the email. Full HTTP inspection ensures no malicious elements are downloaded.
2. Web based email is very common, and users access private email sometimes corporate email accounts via the browser. This mean email is actually Web browsing, web-email should be inspected not just for file downloads of attached files, but with full content inspection, against all Web threats as discussed in this document.

eSafe inspects all popular web email services against all those threats the same way it does all Web surfing traffic – completing the organizational email security.

## **The Core eSafe Security**

### **4-Layer defense against spyware and web surfing attacks**

Unlike other solutions that block spyware by URL, file signature or a combination of both - eSafe blocks Spyware through all its phases.

### **eSafe Content Security Layers Explained**

#### **Layer 1: Content access level blocking**

URL filtering:

- 4 malicious site categories: malware, spam, phishing, virus/hacker/spyware
- 56 other categories, including objectionable sites, and non-productive sites

HTTPS (SSL, TLS) certification validation and authorization(with eSafe Web SSL)

Selective ActiveX blocking:

- Work by white-list: only known “Good” ActiveX are allowed to be downloaded by CLSID
- Work by blacklist: known malicious ActiveX CLSID are blocked
- Work by pre-installed only: ActiveX allowed to run in the browser if already installed, but no ActiveX is allowed to be downloaded (except if the server/domain is on a white-list)

#### **Layer 2: Dynamic web threats**

Today's dynamic threats are embedded within web pages. HTTP 'drive-by' attack protection includes inspection of HTTP headers and request, as well as full HTML inspection of all web and “web 2.0” pages content. This enables to block malicious attacks not only from known malicious sites, but also in the majority of the Internet which is considered a grey security area. It also covers threats in hacked legitimate sites, where content was modified or infected by attackers.

On layer 2 eSafe protects against:

- Zero-day client-side browser vulnerability exploits
- Malicious VB and Java scripts
- Spyware pop-installers and auto-installing dialers

### Layer 3: File analysis

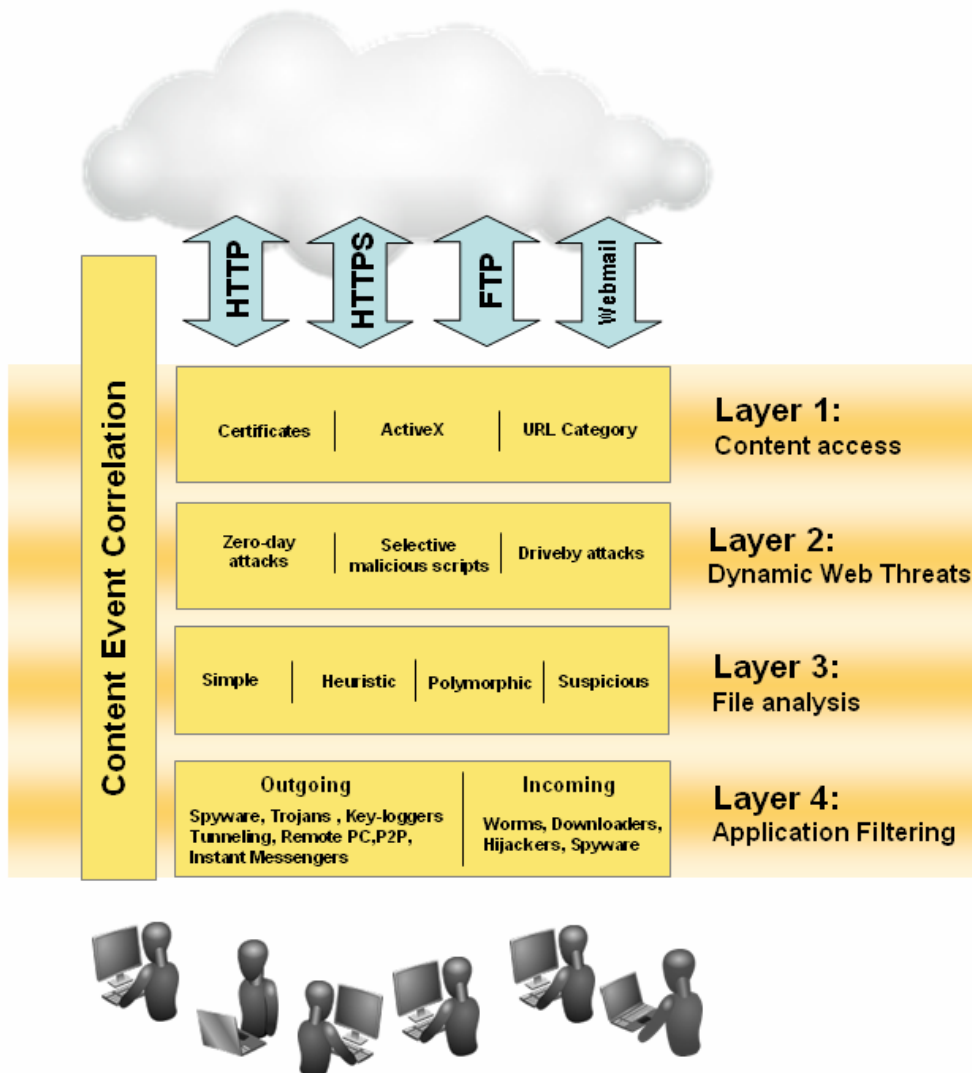
An advanced anti-x security engine inspects binary, executable, Microsoft Office, and compressed archive files against all types of threats: spyware, Trojans, zombie-bots, viruses, worms, rootkits, etc. The engine is certified by ICSA and Checkmark to block 100% ITW (in the wild) threats, and Spyware. The engine contains several technologies which enable it to detect not only known threats but also suspicious files and variants of malicious code from known families. The engine contains the following:

- Simple signatures for specific malicious code
- Smart signatures, using heuristics to detect variants from known families
- Emulation engine to decode and expose polymorphic, stealth and other sophisticated malicious code
- Unique patent pending HOFA™ (Hostile Operation Flow Analysis) technology to detect suspicious spyware / Trojan / worm code

#### Signature Updates

All signatures are timely updated on par with all leading antivirus vendors, even if the malicious code is blocked proactively, which is the case in most situations. The eSafe CSRT (Content Security Response Team) operates 24x7x365 to make sure customers are always protected.

## CSL Model: Content Security Layers (CSL) Model



#### Layer 4: Communications blocking

Communications blocking currently include 18 families of communication patterns, mainly for outbound traffic. Some of these include:

- Outbound spyware and related traffic protocols: spyware, adware, BHO, ad-supported software,
- Inbound spyware and related: browser hijackers, pop-installers, drive-by spyware
- Instant messengers chat (MSN, ICQ/AOL/AIM, Yahoo!, IRC, and more.)
- Instant messengers file transfer
- P2P (various), Skype
- Outbound tunneling
- Protocol enforcement (HTTP, HTTPS, HTTP WebDAV, etc.)
- Remote Control / Remote PC
- Inbound / outbound Internet worms and TCP exploits
- Outbound Trojan and keylogger traffic

### eSafe Compared to Other Perimeter Security Product Categories

A balance between Security, Performance, and User Experience is essential for perimeter security. Changes to this balance results in network impacts, security breaches, or user complaints. eSafe's innovative design and technologies provide perfectly balanced content security. Various types of other perimeter security solutions compromise on various aspects or simply not provide certain necessary content security functionality due to inherent limitation.

#### eSafe compared to Firewalls

A firewall is designed to permit or deny data connections between computer networks with different zones of trust, but does not inspect the content within the connections. Virtually all firewalls allow the basic function of web browsing which means users can access almost any web page no restriction. Compared to firewalls eSafe provides the following content security functionality:

- Inspects all incoming and outgoing content on relevant protocol connections
- Blocks malicious code such as spyware, Trojans, and viruses
- Modifies web content in pages containing suspicious code (selectively removes malicious scripts, exploits, etc.)
- Policy based protocol usage enforcement for various web-enabled applications

#### eSafe compared to IDP (IDS/IPS)

Intrusion Detection and Prevention (IDP) systems are designed to identify network based attacks. These systems can be passive (IDS) or active (IPS). IDS are logging systems and do not provide any active security against content threats.

IPS are monitoring mostly at the network layer and can prevent malicious activities such as denial of service (DoS), port scanning, or malformed packets. They typically do not inspect content at the application layer, nor block malicious code. Their ability to prevent various vulnerabilities and exploits is limited. Various vendors have added more content security capabilities to IPS products, but these impact performance and have other limitations.

Compared to IPS eSafe provides the following content security functionality:

- IPS does not block most malicious code such as spyware, Trojans, and viruses or blocks only certain web worms and some other very specific outbreak samples. eSafe blocks 100% of known malware and over 95% of unknown malware.
- Unlike eSafe, IPS blocking of content threats is limited to simple string patterns. This is effective against very few active content threats such as web page malicious scripts, specific browser, OS, and HTML exploits, etc.

- eSafe can dynamically modify web content in pages containing suspicious code by selectively removing malicious scripts, exploits, etc. without impacting user experience. IPS products that can modify web content either block the entire web page, or block certain elements from all web pages (all scripts, ActiveX, Java applets, etc.) this is simply not acceptable and rarely applied.
- eSafe provides policy based protocol usage enforcement for various web-enabled applications.

### **eSafe compared to UTM**

UTM (Unified Threat Management) are all-in-one security products combining a firewall, VPN, IPS, antivirus, content filtering, and more. Since some of the functionality is very complex the performance is determined by the slowest element which is typically content filtering. As a result UTM products make content security in comparison to eSafe:

- All-in-one - but only “average” content security at best.
- Integrated simple antivirus-engine effective for downloaded files only (EXE, ZIP, etc.)
- Limited deep-web inspection (IPS technology – see above).
- Inadequate for larger and higher-security organizations.

### **eSafe compared to URL filters**

URL Filtering products are designed to block or monitor access to web sites according to category. Most sites categories are effective for productivity enforcement either by blocking access to non-work related or objectionable categories (adult, criminal, etc.) or by monitoring user access. Although some categories are security related and are useful for blocking access to known malicious sites – URL filters should be a part of a more comprehensive solution. Some limitations of URL filtering solutions compared to eSafe:

- Focusing on productivity and contain extensive productivity categories and few security/malicious categories.
- Reactive “blacklists” based - does not “know” all the web. Not effective against targeted attacks. Web analyzing of malicious sites is an exhaustive non real-time data-center activity not effective against dynamically changing malicious sites containing zero-day exploits and targeted Trojan attacks.
- Not effective against malicious code implanted in hacked web sites.
- No deep web inspection or application filtering.
- A simple third party file antivirus engine is optional in some products - effective only against known (by signature) malicious code via directly downloaded.

### **eSafe compared to gateway antivirus**

Gateway antivirus products typically rely on a combination of a simple file antivirus engine and a collection of “blacklist” rules blocking access to a restricted list of known malicious sites. In effect it is similar to URL filtering solutions with the added antivirus engine option. These solutions are based on proxy technology and only inspect downloaded executable files (EXE, ZIP, CAB, etc.). These solutions are reactive, based almost entirely on constant updates with almost no proactivity. The proxy technology itself prevents true transparent inline inspection of all web content.

- Based on multi-purpose (same for desktop and gateway use) antivirus engine technologies. These are reactive technologies designed to cope well with known malicious code – only after it was discovered, analyzed and a signature update made available. eSafe includes multiple layers of security blocking 100% of known malware and over 95% of unknown malware.
- Unlike eSafe's NitroInspection™ real time content inspection, most gateway based antivirus products are based on proxy technologies with its inherent limitations (more information the section *Unique eSafe Capabilities*).

- No deep web inspection or application filtering capabilities.
- Typically difficult to scale-up mostly due to reliance on proxy technologies. In large organizations scalability could be very complex and expensive, relying on third party load balancing hardware.

## **eSafe compared to caching proxy security appliances**

Caching proxy security appliances are very similar to other types of solutions mentioned above and mostly add a file antivirus engine and a URL filtering database to the proxy device and all respective commentary above applies to them as well. Since the proxy server market is slowly growing (if at all) – some proxy server vendors have re-positioned their products as security devices. The major limitation is that in most situations web content (threats in web pages) are not inspected and the content cannot be dynamically modified. In addition, these products are usually much more expensive than other available proxy solutions.

eSafe not only provides improved security and performance but also works perfectly well with all top caching proxy solutions. In fact a customer looking for the best proxy based content security appliance should purchase the caching proxy from the vendor and integrate it with eSafe using the ICAP protocol or eSafe's forwarding proxy mode.

- Requires an expensive non-integrated caching proxy.
- Uses antivirus engine provided by third party vendors. These are reactive technologies designed to cope well with known malicious code – only after it was discovered, analyzed and a signature update made available. eSafe includes multiple layers of security blocking 100% of known malware and over 95% of unknown malware using the certified eSafe content security engine.
- No deep web inspection or application filtering capabilities.
- Limited capacities. Difficult and expensive to scale-up.